2026

Intelligence on Iranian nuclear programme

Pax Consulting

11-04-2026

Index

1. INTRODUCTION

The intelligence conflict surrounding the Iranian nuclear programme represents a multi-generational espionage campaign that has fundamentally reshaped modern statecraft. For decades, the United States, led by the Central Intelligence Agency (CIA) and the National Security Agency (NSA), alongside the United Kingdom's Secret Intelligence Service (MI6) and Government Communications Headquarters (GCHQ), have engaged in an **extensive shadow war against Iran.** This intelligence effort has **transitioned from traditional human-centric "briefcase diplomacy" to highly sophisticated cyber-physical operations,** driven by the shared objective of unmasking, monitoring, and delaying Iran's suspected development of a nuclear weapon.

These agencies have frequently relied on global allies for both human and technical operations. British and American agencies have sought Iranian contacts worldwide, including merchant navy captains, businesspeople, or scientists at Western events, to name a few examples.

2. INTELLIGENCE GATHERING EFFORTS

The United States and Britain have utilized a combination of Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and cyber espionage to penetrate the Iranian nuclear ecosystem.

2.1 HUMINT and defector programmes

Rather than relying exclusively on assassinations **like their Israeli counterparts,** the **CIA prioritized recruiting Iranian nuclear scientists to defect,** offering them protection in exchange for highly classified intelligence.

CIA case officers spent years cultivating relationships with **key Iranian insiders,** such as a founding father of Iran's covert nuclear programme codenamed "Shelve" and another scientist codenamed "Bernadine". These assets provided Western intelligence with **invaluable insights** into Iran's acquisition of blueprints from the Pakistani A.Q. Khan network[1], the scale of Iran's nuclear ambitions, and detailed layouts of secret facilities.

[1] The **A.Q. Khan network** was a massive, illicit international nuclear proliferation ring that operated from the late 1980s until its exposure in 2003. It is widely considered one of the most dangerous nuclear smuggling operations in history. The network was spearheaded by **Abdul**

In a more recent joint HUMINT operation in late 2018, **MI6, the CIA, and Israel's Mossad collaborated to successfully smuggle a defecting Iranian nuclear technician out of the country** and across the English Channel on an inflatable dinghy so he could be debriefed in the UK before being extracted to the US.

2.2 SIGINT and procurement tracking

British intelligence has played a vital role in counter-proliferation by **intercepting illicit procurement networks and enforcing international sanctions.**

In 2007, GCHQ intercepted critical communications that confirmed Iran had halted its weaponization program in 2003, a piece of intelligence that deeply informed Western policy. Furthermore, by flipping members of the A.Q. Khan network—such as **Swiss engineer Urs Tinner**—the CIA and its allies were able to **track the specific components being shipped to Iran.**

This procurement tracking, combined with high-resolution satellite imagery, **enabled the US, UK, and France to discover the clandestine underground enrichment plant at Fordow in 2009** long before Iran officially declared it.

2.3 Cyber espionage

To map Iranian networks, the US and Israel **infiltrated Iranian computers** using highly sophisticated espionage malware like *Flame*, which compromised the Iranian Oil Ministry to steal documents, scan for devices, and record conversations. This surveillance paved the way for larger sabotage operations like *Stuxnet* and the contingency cyber-warfare plan *Nitro Zeus.*

Flame was one of the most complex and **massive pieces of espionage malware** ever found. The target were Government organizations, educational institutions, and private individuals primarily in Middle Eastern countries, **heavily concentrated in Iran.** Flame was built purely for intelligence gathering.

Stuxnet is widely considered the world's first true cyber weapon because it was the first known malware

---

Qadeer Khan (A.Q. Khan), a Pakistani metallurgist and physicist known as the "father" of Pakistan's nuclear bomb. Iran, North Korea and Libya enjoyed its services.

designed to cause physical destruction to real-world infrastructure. **The target was Iran's Natanz nuclear enrichment facility** (which, notably, was built using centrifuge designs acquired from the A.Q. Khan network).

Unlike Stuxnet and Flame, **Nitro Zeus** was not a single piece of malware; it was a **massive, comprehensive cyber warfare contingency plan** developed by the U.S. military. **Nitro Zeus was designed as a fallback option in case diplomatic efforts to stop Iran's nuclear program failed and the U.S. found itself in a military conflict with Iran.** It was designed to **paralyze Iran without firing a physical shot.** U.S. Cyber Command successfully infiltrated and placed hidden implants ("backdoors") deeply within Iranian critical infrastructure.

3. ASSESSMENT OF THE SUCCESS OF INTELLIGENCE EFFORTS

The combined intelligence-gathering efforts provided the US and its allies with an **exceptionally comprehensive understanding of Iran's nuclear program.** Former US officials noted that the CIA achieved "tremendous penetration" into Iranian facilities, down to possessing actual architectural blueprints. **This deep intelligence directly facilitated the 2010 Stuxnet cyberattacks, secured the diplomatic confidence needed for the 2015 JCPOA nuclear deal, and allowed the Pentagon to construct life-size underground facsimiles of the Natanz, Fordow, and Isfahan facilities** to train US Special Forces and plan future bombing raids, which the world saw very recently on **June 22, 2025,** under the Trump administration.

Despite these triumphs, the intelligence campaign suffered devastating setbacks. One of the most disastrous failures occurred when **a rudimentary, web-based CIA communication system used to manage Iranian spies was exposed via "Google Dorks"** (advanced search queries).

After a tip from a double agent, Iranian intelligence systematically used Google to locate the CIA's hidden websites, **unravelling the entire espionage network between 2009 and 2013, which resulted in the imprisonment and execution of dozens of American sources.**

Another notable failure was **"Operation Merlin" in 2000,** where **the CIA deliberately provided Iran with flawed nuclear warhead blueprints in an attempt to sabotage their progress;** the **Russian courier, codename Merlin,** exposed

the flaws to the Iranians, potentially **providing Tehran with valuable technical insights rather than hindering them.**

Merlin was a Russian émigré and a former senior nuclear engineer. He had worked at **Arzamas-16**, the Soviet Union's equivalent of Los Alamos and the heart of their nuclear weapons design programme. **The CIA contacted him in the mid-1990s** because he had the perfect profile: he possessed highly specialized knowledge of nuclear "firesets" (the complex explosive mechanisms required to trigger a nuclear detonation) and **could credibly pose as a disgruntled Russian scientist looking to sell state secrets for cash.**

The CIA sketched flawed blueprints which were going to be delivered by Merlin. Because he was an actual expert in nuclear physics, he immediately spotted that the blueprints were wrong. Crucial components were missing from the diagrams, and the parts list was written in English rather than Russian. **He warned his handlers, stating bluntly, "This won't work".** And it didn't.

In March 2000, **Merlin travelled to Vienna, Austria, to deliver the package to the Iranian mission.** Feeling highly skeptical of the plan and terrified that the Iranians would realize they were being scammed (**which could put his life in danger**), he went off-script.

Before sliding the blueprints through the mail slot of the Iranian mission (he avoided a face-to-face meeting), **Merlin inserted a personal letter into the package. In the letter, he explicitly warned the Iranians that the blueprints were incomplete and pointed out exactly where the flaws and missing parts were.**

Operation Merlin may have achieved the exact opposite of its goal. By pointing out the flaws, Merlin essentially gave Iranian scientists a highly advanced, functional Russian blueprint that they could compare against other black-market designs (like those acquired from the A.Q. Khan network).

4. ATTACKS ON MAIN NUCLEAR INSTALLATIONS

Over the past year, the intelligence conflict escalated into direct kinetic warfare. In June 2025 ("Operation Midnight Hammer") and February 2026 ("Operation Epic Fury" and Israel's "Roaring Lion"), the US and Israel launched massive military strikes against Iran's heavily fortified nuclear installations at **Natanz, Fordow, and Isfahan.** Utilizing Massive Ordnance Penetrators (bunker-buster bombs), the US Air Force successfully penetrated underground tunnels, heavily damaged centrifuge enrichment halls, and destroyed uranium conversion lines.

This topic has been largely discussed in our blog in June 2025[2].

Despite the sheer physical devastation of these facilities, **Iran retains a stockpile of approximately 400 to 409[3] kilograms of highly enriched uranium (HEU) purified to 60 percent.**

It is unknown where this materiel has been placed although it is likely to have been dispersed in different installations **in order to prevent attacks from being successful at destroying all of it.**

Following the strikes, the International Atomic Energy Agency (IAEA) lost control and visibility over this uranium. Intelligence experts assess that while **industrial-scale enrichment has been set back by years**, Iran could theoretically execute a rapid weaponization effort within one to two years.

However, **it is thoughtful to assess that the US and Israel still enjoy intelligence capabilities from within** and it could help explain some of the latest attacks. For instance, between March 24th and April 1st, 2026, a former installation (Shahid Boroujerdi) of an old nuclear programme called AMAD[4] dismantled falsely in 2003, was bombed.

The site was built under a mountain within the Parchin military complex and features two tunnel entrances and above-ground support buildings. Although believed to be abandoned, the attack on this location infers that available intelligence (whether US or Israeli) indicated **the installation had been reactivated to serve Iranian nuclear ambitions.**

5. CONCLUSIONS

The so-called anglosphere intelligence agencies have worked for decades in the search and acquisition of information

[2] https://paxconsulting.blog/2025/06/25/iran-way-forward/

[3] This amount was estimated before the attacks in June 2025.

[4] A highly classified, covert Iranian scientific and military project initiated in the late 1980s with the explicit goal of developing a nuclear arsenal. Led by Iranian physicist Mohsen Fakhrizadeh, the program specifically aimed to design, produce, and test five 10-kiloton nuclear warheads and integrate them onto ballistic missiles (like the Shahab-3). While international intelligence agencies and the IAEA assess that the coordinated military program was officially halted in late 2003 under international pressure, a massive trove of documents seized by Israeli Mossad agents in 2018 (the "Nuclear Archive") confirmed the project's extensive scope. The archive also revealed that after 2003, the AMAD Plan's research, blueprints, and personnel were decentralized and shifted into other covert defence organizations to preserve Iran's nuclear weaponization know-how.

regarding the Iranian nuclear programme in conjunction with missile programmes. Both are intertwined as a nuclear bomb is useless if no vector of deployment is available.

Achievements and setbacks have been acknowledged over the years. However, more recently established capabilities remain unknown, otherwise it could potentially endanger lives in Iran.

Current events show that the US and Israel count on troves of intelligence regarding the nuclear programme, defence installations, missile programmes and capabilities to locate and annihilate main figures of the regime, as well as IRGC leaders, scientists, prominent C3I (command, control, communications and intelligence) individuals and installations. **It involves human and technical assets that have been operating for years prior to the attacks and remain active in efforts to topple the regime.**

What seems to have failed so far is the readiness of the **local population to rise up against their leaders**, or a **failure to gauge** the repression capabilities of the regime and its will to survive.

The rift between IRGC leadership and the government is apparent and profound. That cleavage is key to fostering any chance of success in negotiations.

The available information indicates that Iran was actively determined to build the bomb while **deceiving its neighbours and the IAEA.** And Iran has done it for decades. Enriching 60% enriched Uranium up to military grade (90%) is far easier and cheaper than enriching yellow cake (raw material) up to 5% (use in nuclear plants).

Therefore, it should be assessed that Iran represents a threat. Considering the lack of check and balances of a regime such as the ayatollah's, advice that it should be prevented from any access to nuclear weapons by all means. It would increase the chances of reckless war in the region with devastating effects for the whole world.

The current state of affairs is often viewed as the lesser of two difficult scenarios: a limited conventional military clash or the growing threat of a nuclear conflict. This dynamic is especially complex given that Iran's nuclear programme remains **under the direct oversight of the Islamic Revolutionary Guard Corps (IRGC).** While some argue that military action could have been delayed to allow more time for diplomatic channels, others point out that **decades of negotiations have yet to yield a permanent resolution.**

Critics of these prolonged diplomatic efforts argue that they have **inadvertently afforded Iran the time to enrich**

uranium to 60%—a level significantly higher than the 20% threshold typically required for medical use. Consequently, **the central policy debate revolves around the strategic risks of allowing the enrichment process to reach military-grade capability before taking decisive action.**

The IAEA currently assesses that roughly 200 kilograms of highly enriched uranium are likely stored in fortified underground tunnels near Isfahan, Natanz, and Fordow. (This figure contrasts with some intelligence agency estimates, which place the stockpile closer to 400 kilograms). The presence of this material raises intense chemical and radiological safety concerns should these storage canisters be breached by bunker-buster munitions. Furthermore, the IAEA has explicitly noted that **its inspectors have been largely unable to verify the status or exact location of these near-weapons-grade stockpiles** since the initial strikes severely degraded Iran's nuclear program in mid-2025.

Given the IAEA's acknowledged loss of ground-level visibility, policymakers and defence analysts must increasingly rely on the classified assessments generated by intelligence agencies such as the CIA and Mossad. While the general public lacks access to this classified data, the visibility limits confirmed by international watchdogs highlight why **these specialized intelligence frameworks remain a necessary tool for evaluating the true extent of the nuclear threat.**